CRYPTOME

Donate for the Cryptome archive of files from June 1996 to the present

---

21 September 2014

Apple and Spy Disbelief

John Gilmore on Apple disbelief:

http://cryptome.org/2014/09/apple-wiretap-disbelief.htm

Google and Apple Subverting Device Encryption?:

http://cryptome.org/2014/09/google-apple-crypto.pdf

Date: Sun, 21 Sep 2014 05:46:57 +0000
From: Jacob Appelbaum <jacob[at]appelbaum.net>
To: John Denker <jsd[at]av8n.com>
Cc: cryptography[at]metzdowd.com
Subject: Re: [Cryptography] new wiretap resistance in iOS 8?

On 9/20/14, John Denker <jsd[at]av8n.com> wrote:
> On 09/19/2014 09:16 PM, John Gilmore wrote:
>> There must be some other reason, I'm just having trouble thinking of it.
>
> 1) As the proverb says, don't let the perfect be the
> enemy of the good.
>
> There will never be perfect security. The measure
> of good security is that it imposes a cost on the
> attacker, out of proportion to the cost borne by
> the user.

I like that proverb but it assumes a baseline standard of good. I think John (Gilmore) is correct to not fall for the marketing hype. It is false to say that the measure here is imposing a cost on the attacker - how do you plan to verify that? How do you know what cost it would impose?

I agree that good is better than none. I might even agree that that we'll never reach perfect, so it is better to have good rather than obviously bad. I don't however agree that this is good as that remains to be seen.

Please do consider that they are described as an NSA PRISM partner. Please do consider that they do appear to have recently lost their warrant cannary.

> The new practice of /not/ escrowing the keys to iOS
> user data does not make the device attack-proof,
> but it does raise the cost of the attack.

How do you know that they don't escrow? We don't know more than what they claim. Furthermore - do you need to escrow keys to mount an attack? I suspect no.

> Forsooth, if this initiative fails, it will not
> be because it didn't sufficiently raise the cost
> to the attackers, but rather because it imposed
> too much burden on the rightful users.

Or perhaps it wasn't anything from the start?

> 2) Another proverb goes even farther in the same
> general direction: A journey of 100 miles begins
> with a single step.
>
> Suppose there is a weakest-link situation, e.g.

> where locking the front door has no measurable
> benefit until you also lock the back door, side
> door, windows, et cetera. You still ought to lock
> the front door! Even if you can't do everything
> at once, take the first step and then proceed
> from there.

If the crypto is bad or if the keys are weak - how will you know that you've been bamboozled?

> 3) It is a mistake to focus too directly on the
> threat from the NSA.

That is a bizarre statement.

The threat from the NSA is the same threat as from anyone with similar capabilities. Consider that the NSA is tasked with compromising an iPhone deployed in Qatar. Consider that they are the adversary that rather than helping Apple, they have traditionally attacked Apple. And no, it doesn't matter if you're a US citizens or a US company.

> Not escrowing the keys makes Apple somewhat less
> of a target for the FSB, Third Directorate, etc.
> etc. etc. etc. Not zero target, but less of a
> target.

Just to settle this - Apple has signing keys. They keep those. They use them to issue updates. They might not be escrowing *your* keys or they might be doing something different. The protocols aren't open or documented, we can't implement free and open clients that we can verify. As Gilmore has rightfully pointed out, they have the capacity to move and you suggest that they won't move when pushed? Consider the case of Yahoo and the proposed fines?

> If you're worried about Apple Headquarters being
> compelled to subvert your phone, you should also
> be worried about a Clipper-like back door in the
> hardware, which is made in China. Ditto for HTC
> and other brands.

I'm worried about all of those things but Apple headquarters is of course the PRISM partner - your other comments are speculation. It is well founded, I agree with it and I don't dismiss it either. Still - here we have evidence of PRISM and Apple's complicity or victimization. Just above you suggest that the enemy of the perfect is the enemy of good enough - it may not be perfect, HTC phones may also be weakened by someone - but if it isn't the NSA, I'd be happy with that as a good solution. Especially since Apple products aren't made by HTC. :-)

> Probably the biggest threat from the NSA is more
> /indirect/. I am referring to weakening crypto
> standards and products, again and again over the
> years, thereby creating conditions for a Hobbesian
> war of all against all. For example, IMHO it was
> both arrogant and stupid for the NSA to think they
> would be the only ones who could break 56-bit DES.

Probably the biggest threat from the NSA is that they'll feed your location data to people who operate drone strikes. Using your nice iPhone, they'll assist in murdering you.

And yes, they also backdoor crypto, actively exploit software and hardware bugs.

To that end - the Hobbesian world is already here. With Apple's help, no less. Is it willing? How would we know? Is it coerced? How can we verify? Absent all of that - you suggest that we... trust?

> Tangential remark: Interesting reference:
> Michael Schwartzbeck
> "The Evolution of US Government Restrictions on
> Using and Exporting Encryption Technologies"
> From "Studies in Intelligence" (the secret internal CIA magazine)
> (date not obvious; circa 1998)
> http://www.foia.cia.gov/sites/default/files/DOC_0006122418.pdf
> (prettier)
> http://www.foia.cia.gov/sites/default/files/DOC_0006231614.pdf (same, but
> uglier)
>
> Also: CIA FOIA homepage (with search feature)
> http://www.foia.cia.gov/

> Hundreds of "Studies in Intelligence" articles
> were released last week.

I'd encourage a read of http://freesnowden.is/ for a healthy dose documents produced by the government for internal information exchange. I love FOIA but I love Snowden's FOIA process a lot more.

> 4) It's bad practice to support a strong argument
> with a weak one, but since the topic has already
> been brought up, let me address it.
>
> For the /subset/ of the problem that concerns
> NSA versus Apple, laws matter ... somewhat. Yes,
> there is a long track record of violations, but
> in the spirit of item (1) above, forcing the NSA
> to resort to lawless and unconstitutional methods
> raises the cost to them.

They're spies. They are lawless. At best they claim these days that an executive order is the same as a law enacted by Congress. They are literally claiming that EO12333 allows them to do dragnet collection. I've had a senior NSA person tell me that EO12333 allows NSA to collect on the Tor network in the US and outside without exception. This has cost them nothing. Alexander, Clapper and others are all free. They are not punished - they are part of a culture of impunity.

The NSA and other "Intelligence Community" members have been doing this for longer than I've been alive. They've been getting caught for ages and no reform has changed anything except in public perception that it is happening at all. It costs them nothing and has cost them nothing.

> In particular, if I have information about you,
> I can be subpoenaed to produce it. However, if
> I don't have the information, I cannot easily
> be compelled to break into your house to collect
> it. If somebody wants to break into your house
> badly enough they can do it, but we can take
> steps to raise the cost.

You can however be jailed for failing to produce information if say, a Grand Jury, believes that you have it. You can be threatened with ever expanding fines as Yahoo was by the FISA "court" process. Again, this argument you're making misses the point by a country mile - the State will put a boot on your neck and you will choke. With a person, it is hard to do that silently. With technology, it costs them nothing and if you're not checking, you might not even notice. And to Gilmore's point, how will you check?

> 5) We agree that illusory security is worse than
> none. Tom Mitchell pointed out yesterday that
> Apple does not want to be "directly" complicit
> in pillaging your data. However ... if pillage
> is still going on, a big pretense of security
> would be worse than nothing. It would reflect
> a "Not My Job" attitude:
> https://www.av8n.com/physics/not-my-job.htm
>
> So I say let's take a step in the right direction
> today ... and then take whatever additional steps
> are necessary.

Open the protocols, free the implementations, discuss the legal situations, deploy end to end crypto where a user is the only person with a key, use ephemeral keys and then address each of the points that Gilmore made.

But whatever is done - let us not remove the pressure - we need more transparency and above all, we need accountability. To shift from PRISM partner to thumbing their nose at their partners suggests that they may turn again.

Wiretapped along with the rest of you,

Jacob
